# On two families of binary quadratic bent functions*

J. Rifà[1], V. A. Zinoviev[2]

November 26, 2012

**Abstract**

We construct two families of binary quadratic bent functions in a combinatorial way. They are self-dual and anti-self-dual quadratic bent functions, respectively, which are not of the Maiorana-McFarland type.

**Keywords** Bent function, combinatorics, quadratic function, self-dual bent function.

**Mathematics Subject Classification (2000)** 94C30; 94C10

## 1 Introduction

Let $\mathbb{F}_q$ be the Galois field of order $q = 2^m$. We use the standard notation $[n, k, d]$ for a binary linear code $C$ of length $n$, dimension $k$ and minimum (Hamming) distance $d$. Denote by $\mathrm{wt}(\mathbf{x})$ the Hamming weight of a vector $\mathbf{x}$ from $\mathbb{F}_2^n$. For $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ denote by $\mathbf{x} \cdot \mathbf{y}$ the usual inner product over $\mathbb{F}_2$. Denote by $\bar{\mathbf{x}}$ the complementary vector of $\mathbf{x}$ (obtained by swapping 0 and 1).

*This work has been partially supported by the Spanish MICINN under Grants MTM2009-08435, by the Catalan AGAUR under Grant 2009SGR1224 and also by the Russian fund of fundamental researches 12-01-00905.

[1]J. Rifà is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain. (email: josep.rifa@uab.cat)

[2] V. A. Zinoviev is with the Institute for Problems of Information Transmission, Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 127994, Russia (e-mail: zinov@iitp.ru).

Let $m \geq 2$ be an integer and $j \in \{0,1,2,3\}$. Denote by $S(j)_m$ the following sum:

$$S(j)_m \;=\; \sum_{k=0,\ldots,m:\ k\equiv j \pmod 4} \binom{m}{k}. \tag{1}$$

Denote by $S(i_1,i_2)_m$ the value $S(i_1,i_2)_m = S(i_1)_m + S(i_2)_m$, for any two different $i_1$ and $i_2$ from $\{0,1,2,3\}$. The next proposition was used in [2] and gives all the values $S(j)_m$ and, hence, the values of all the sums $S(i_1,i_2)_m$, which we will use later.

**Proposition 1.1** *[2] For any $m \geq 2$ denote $B_m = 2^{s-1}$, where $s = \lfloor \frac{m}{2} \rfloor$. Then, the values of $S(j)_m$ depending on $m \equiv 0,1,2,3,4,5,6,7 \pmod 8$ are, respectively:*

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $S(0)_m$ = | $B_m^2 + B_m$ | $2B_m^2 + B_m$ | $B_m^2$ | $2B_m^2 - B_m$ | $B_m^2 - B_m$ | $2B_m^2 - B_m$ | $B_m^2$ | $2B_m^2 + B_m$ |
| $S(1)_m$ = | $B_m^2$ | $2B_m^2 + B_m$ | $B_m^2 + B_m$ | $2B_m^2 + B_m$ | $B_m^2$ | $2B_m^2 - B_m$ | $B_m^2 - B_m$ | $2B_m^2 - B_m$ |
| $S(2)_m$ = | $B_m^2 - B_m$ | $2B_m^2 - B_m$ | $B_m^2$ | $2B_m^2 + B_m$ | $B_m^2 + B_m$ | $2B_m^2 + B_m$ | $B_m^2$ | $2B_m^2 - B_m$ |
| $S(3)_m$ = | $B_m^2$ | $2B_m^2 - B_m$ | $B_m^2 - B_m$ | $2B_m^2 - B_m$ | $B_m^2$ | $2B_m^2 + B_m$ | $B_m^2 + B_m$ | $2B_m^2 + B_m$ |

A *boolean function* $f$ in $m$ variables is any map from $\mathbb{F}_2^m$ to $\mathbb{F}_2$. The *weight* of a boolean function $f$ denoted by $\mathrm{wt}(f)$ is the Hamming weight of the binary vector of the values of $f$, i.e., the number of $\mathbf{x} \in \mathbb{F}_2^m$ such that $f(\mathbf{x}) = 1$. For any boolean function $f$ we define its Walsh-Hadamard transform $F$, such that

$$F(\mathbf{a}) \;=\; \sum_{\mathbf{x}\in\mathbb{F}_2^m} (-1)^{f(\mathbf{x})+\mathbf{a}\cdot\mathbf{x}}, \;\; \forall\, \mathbf{a} \in \mathbb{F}_2^m. \tag{2}$$

For even $m$, a boolean function $f$ over $\mathbb{F}_2^m$ is *bent* if its Walsh-Hadamard transform is $F(\mathbf{y}) = \pm 2^{m/2}$, for all $\mathbf{y} \in \mathbb{F}_2^m$.

Two boolean functions $f, g$ are *affine equivalent* if there exists a linear map $A \in GL(m,\mathbb{F}_2)$, $\mathbf{b},\mathbf{c} \in \mathbb{F}_2^m$ and $\epsilon \in \mathbb{F}_2$ such that$g(\mathbf{x}) = f(A(\mathbf{x}) + \mathbf{b}) + \mathbf{c}\cdot\mathbf{x} + \epsilon$, where $\mathbf{c}\cdot\mathbf{x}$ is the inner product of $\mathbf{c}$ and $\mathbf{x}$.

It is well known that the Walsh-Hadamard transform $F$ of a bent function $f$ defines a new bent function $\tilde{f}$, such that $F(\mathbf{y}) = 2^{m/2}(-1)^{\tilde{f}(\mathbf{y})}$. The function $\tilde{f}$ is called the *dual* of $f$ and it is fulfilled that $\tilde{\tilde{f}} = f$. We take the following definitions from [3].

**Definition 1.2** *[3] A bent function $f$ is called self-dual, if it is equal to its dual. It is called anti-self-dual, if it is equal to the complement of its dual.*

In this quoted paper [3], all self-dual bent functions in $m \leq 6$ variables and all quadratic such functions in $m \leq 8$ variables are characterized, up to a restricted form of affine equivalence. Later, Hou [5] classified all self-dual and anti-self-dual quadratic bent functions under the action of the orthogonal group $O(m, \mathbb{F}_2)$.

A general class of bent functions is the *Maiorana-McFarland* class, that is, functions of the form

$$\mathbf{x} \cdot \varphi(\mathbf{y}) + g(\mathbf{y}), \tag{3}$$

where $\mathbf{x}, \mathbf{y}$ are binary vectors of length $m/2$, $\varphi$ is any permutation in $\mathbb{F}_2^{m/2}$, and $g$ is an arbitrary boolean function.

One of the open questions concerning self-dual bent and anti-self-dual bent functions is the following one, quoted in [3]: *are there quadratic self-dual (anti-self-dual) bent functions which are not of Maiorana-McFarland type?*

In the present paper we give infinite families of self-dual and anti-self-dual quadratic bent functions which are not of the Maiorana-McFarland type. Since our class of bent functions includes not only self-dual and anti-self-dual quadratic bent functions we think that our class of bent functions is interesting itself and also from the point of view of secondary constructions [3]. The material is organized as follows. In Section 1 we introduce the topic and give notations and preliminary results. Section 2 contains the new constructions of quadratic bent functions and the main results of the paper.

# 2 A combinatorial construction of new bent functions

Throughout this section we assume that $m$ is even.

Denote by $H_m$ the parity check matrix of the binary

Hamming code of length $n = 2^m - 1$ and by $H_m^*$ denote the matrix obtained from $H_m$ by adding one zero column.

For a given even $m \geq 4$ and any $i_1, i_2 \in \{0, 1, 2, 3\}$, where $i_1 \neq i_2$, denote by $\mathbf{v}_{i_1,i_2} = (v_0, v_i, ..., v_{n-1})$ the binary vector whose $j$-th position $v_j$ is a function of the value of weight of

the column $\mathbf{h}_j$ in $H_m^*$:

$$v_j = \begin{cases} 1, & \text{if} \quad \mathrm{wt}(\mathbf{h}_j) \equiv i_1 \text{ or } i_2 \pmod 4 \\ 0, & \text{otherwise.} \end{cases}$$

The next result is part of a proposition in [2] and proved there.

**Proposition 2.1** *[2] Let $m$ be even and let $\mathcal{H}_m^*$ be an extended Hamming code of length $2^m$. Then, the values of weights of vectors in the coset $\mathbf{v}_{i_1,i_2} + (\mathcal{H}_m^*)^\perp$ are $2^{m-1} \pm 2^{\frac{m}{2}-1}$, if and only if $i_1 - i_2 \equiv 1 \pmod 2$.*

For a given even $m \geq 4$ and any $i_1, i_2 \in \{0,1,2,3\}$, where $i_1 \neq i_2$, define the boolean function $f_{i_1,i_2}$ over $\mathbb{F}_2^m$ as:

$$f_{i_1,i_2}(\mathbf{x}) = \begin{cases} 1, & \text{if} \quad \mathrm{wt}(\mathbf{x}) \equiv i_1 \text{ or } i_2 \pmod 4 \\ 0, & \text{otherwise.} \end{cases}$$

Now we state one of the main results of the present paper.

**Theorem 2.2** *For any even $m$, $m \geq 4$ the function $f_{i_1,i_2}$ is a bent function if and only if $i_1 - i_2 \equiv 1 \pmod 2$. In these cases, when $f_{i_1,i_2}$ is a bent function it is a quadratic bent function.*

*Proof.* From Proposition 2.1 the function $f_{i_1,i_2}$ is bent if and only if $i_1 - i_2 \equiv 1 \pmod 2$. Now, we show that all these bent functions are quadratic. Specifically,

$$\begin{aligned} f_{2,3}(x_1, x_2, \ldots, x_m) &\equiv \sum_{1 \leq i < j \leq m} x_i x_j \pmod 2 \\ f_{1,2}(x_1, x_2, \ldots, x_m) &\equiv \sum_{1 \leq i \leq m} x_i + \sum_{1 \leq i < j \leq m} x_i x_j \pmod 2 \\ f_{0,1}(x_1, x_2, \ldots, x_m) &\equiv 1 + f_{2,3}(x_1, x_2, \ldots, x_m) \pmod 2 \\ f_{0,3}(x_1, x_2, \ldots, x_m) &\equiv 1 + f_{1,2}(x_1, x_2, \ldots, x_m) \pmod 2 \end{aligned}$$

To prove the first equality is equivalent to prove that $\binom{w}{2} \equiv 1 \pmod 2$ if and only if $w \equiv \{2,3\} \pmod 4$, where $w$ is an integer number, $0 \leq w \leq m$. Hence, it is enough to prove that for $w \in \{0,1,2,3\}$, we have $\binom{w}{2} \equiv 1 \pmod 2$ if and only if $w \in \{2,3\}$, which is clear.

The second equality is reduced to prove that for $w \in \{0,1,2,3\}$, we have $w + \binom{w}{2} \equiv 1 \pmod 2$ if and only if $w \in \{1,2\}$, which is also clear.

The last two equalities come from the two first.

Following [4, Ch. 15, §2], we can write a quadratic boolean function as $f(\mathbf{x}) = \mathbf{x}Q\mathbf{x}^T + L\mathbf{x} + \epsilon$ and, for the above functions we have:

$$\begin{aligned} f_{2,3}(\mathbf{x}) &= \mathbf{x}Q\mathbf{x}^T, \\ f_{1,2}(\mathbf{x}) &= \mathbf{x}Q\mathbf{x}^T + L\mathbf{x}^T, \\ f_{0,1}(\mathbf{x}) &= \mathbf{x}Q\mathbf{x}^T + \epsilon, \\ f_{0,3}(\mathbf{x}) &= \mathbf{x}Q\mathbf{x}^T + L\mathbf{x}^T + \epsilon, \end{aligned} \tag{4}$$

where $Q$ is the all ones upper triangular binary $m \times m$ matrix with zeroes in the diagonal, $L$ is the all ones binary vector of length $m$ and $\epsilon = 1$. □

**Proposition 2.3** *Bent function $f_{0,1}$ is complementary (hence, affine equivalent) to $f_{2,3}$, as well as $f_{0,3}$ is complementary (affine equivalent) to $f_{1,2}$. Bent functions $f_{0,1}$ and $f_{0,3}$ are affine equivalent to each other, if and only if $m$ is a multiple of 4.*

*Proof.* The fact that $f_{0,1}$ is complementary to $f_{2,3}$, as well as $f_{0,3}$ is complementary to $f_{1,2}$, comes from the definition of these functions.

Consider the functions $f_{0,1}, f_{0,3}$ and define the map $\varphi : \mathbb{F}_2^m \to \mathbb{F}_2^m$, which swaps zeroes and ones of binary vectors $\mathbf{x}$ of length $m$, so $\varphi(\mathbf{x}) = \mathbf{x} + \mathbf{u} = \bar{\mathbf{x}}$, where $\mathbf{u}$ is the all ones vector in $\mathbb{F}_2^m$. Then, $f_{0,1}(\mathbf{x}) = f_{0,3}(\bar{\mathbf{x}})$ if and only if $m$ is a multiple of 4. Indeed, let $\mathrm{wt}_4(\mathbf{x})$ be the weight of $\mathbf{x}$ modulo 4. We have $f_{0,1}(\mathbf{x}) = 1$ if and only if $\mathrm{wt}_4(\mathbf{x}) \in \{0,1\}$ and $f_{0,3}(\bar{\mathbf{x}}) = 1$ if and only if $\mathrm{wt}_4(\mathbf{x}) \in \{m_4, (m-3)_4\}$, where $m_4, (m-3)_4$ stands for the value, modulo 4, of $m$ and $m-3$, respectively. Now is clear that $\{0,1\} = \{m_4, (m-3)_4\}$ if and only if $m$ is a multiple of 4. □

We have to notice that the function $f_{0,1}$ and its complementary $f_{2,3}$ has been constructed in [6] in terms of abelian difference sets, known also as Menon difference sets (see [1]). Since

functions $f_{0,1}$ and $f_{0,3}$ are not equivalent to each other when $m$ is not a multiple of 4, it might be interesting their study from the point of view of difference sets.

**Theorem 2.4**

*For $m \equiv 0, 4 \pmod 8$, the functions $f_{i_1,i_2}$ are neither self-dual functions nor anti-self-dual.*

*For $m \equiv 2 \pmod 8$, $f_{2,3}$ and $f_{0,1}$ are self-dual. The function $f_{0,3}$ is anti-self-dual (with $f_{1,2}$).*

*For $m \equiv 6 \pmod 8$, $f_{1,2}$ and $f_{0,3}$ are self-dual. The function $f_{2,3}$ is anti-self-dual (with $f_{0,1}$).*

*Proof.* It is known [3, Th. 4.1] that if $f$ is a self-dual bent or anti-self-dual bent quadratic boolean function then the symplectic matrix $Q + Q^T$ associated to $f$ (4) is an involution, hence $(Q + Q^T)^2 = I$ ($I$ is the identity matrix of order $m$). Later, Hou [5, Th. 2.1], extended this property to a necessary and sufficient condition in the sense that $f$ is self-dual or anti-self-dual if and only if $(Q + Q^T)^2 = I$, and $(Q + Q^T)Q(Q + Q^T) + Q^T$ is an alternating matrix (so, a matrix of the form $A + A^T$, where $A$ is a square matrix over $\mathbb{F}_2$).

In all cases of our functions $f_{i_1,i_2}$ the symplectic matrix $Q + Q^T$ coincides with $J + I$, where $J$ is the $m \times m$ matrix with ones in all the entries and $Q$ is the all ones upper triangular binary $m \times m$ matrix with zeroes in the diagonal (4).

Hence, $(Q + Q^T)^2 = (J + I)^2 = J^2 + I = I$ (the last equality is true since $m$ is even).

For the second condition we have

$$\begin{aligned} & (Q + Q^T)Q(Q + Q^T) + Q^T \\ = \; & (J + I)Q(J + I) + Q^T \\ = \; & JQJ + JQ + QJ + Q + Q^T \\ = \; & \binom{m}{2} J + JQ + QJ + Q + Q^T. \end{aligned}$$

Taking into account that $m$ is even we see that $\binom{m}{2} J$ is the zero matrix if and only if $m \equiv 0 \pmod 4$. In all other cases $\binom{m}{2} J = J$. We also have $JQ + QJ = (a_{ij})$, where $a_{ij} = 1$ when $i + j$ is even and $a_{ij} = 0$ when $i + j$ is odd. Therefore, $JQ + QJ = A + A^T + I$, for some $A$.

Finally,

$$\begin{aligned}
& (Q+Q^T)Q(Q+Q^T)+Q^T \\
= & \binom{m}{2}J + A + A^T + I + Q + Q^T \\
= & \binom{m}{2}J + (A+Q) + (A+Q)^T + I,
\end{aligned}$$

which is an alternating matrix if and only if $m \not\equiv 0 \pmod 4$ and so, we conclude that $f_{i_1,i_2}$ is a self-dual or anti-self-dual quadratic bent function if and only if $m \not\equiv 0 \pmod 4$.

Now that we know in what cases $f_{i_1,i_2}$ is a self-dual or anti-self-dual quadratic bent function we can check the self-duality or anti-self-duality condition, for each pair $(i_1, i_2)$. It is not necessary to check that the dual bent function $\tilde{f}_{i_1,i_2}$ coincides with $f_{i_1,i_2}$ or with the complement $\bar{f}_{i_1,i_2}$, it is enough to check if the first coordinate in $f_{i_1,i_2}$ coincides with the first coordinate in $\tilde{f}_{i_1,i_2}$ to decide about self-duality or anti-self-duality.

Let us begin by computing

$$F_{i_1,i_2}(\mathbf{0}) = \sum_{\mathbf{x}\in\mathbb{F}_2^m} (-1)^{f_{i_1,i_2}(\mathbf{x})+\mathbf{0}\cdot\mathbf{x}} = \sum_{\mathbf{x}\in\mathbb{F}_2^m} (-1)^{f_{i_1,i_2}(\mathbf{x})} = 2^m - 2\mathrm{wt}(f_{i_1,i_2})$$

and note that $\mathrm{wt}(f_{i_1,i_2})$ depends on the value of the pair $(i_1, i_2)$.

Using Proposition 1.1 we have the following values for $\mathrm{wt}(f_{i_1,i_2}) = S(i_1)_m + S(i_2)_m$, where $B_m = 2^{(m-2)/2}$ :

| $\mathrm{wt}(f_{i_1,i_2})$ | $m \equiv 2 \pmod 8$ | $m \equiv 6 \pmod 8$ |
|---|---|---|
| $(i_1, i_2) = (0, 1)$ | $2B_m^2 + B_m$ | $2B_m^2 - B_m$ |
| $(i_1, i_2) = (2, 3)$ | $2B_m^2 - B_m$ | $2B_m^2 + B_m$ |
| $(i_1, i_2) = (0, 3)$ | $2B_m^2 - B_m$ | $2B_m^2 + B_m$ |
| $(i_1, i_2) = (1, 2)$ | $2B_m^2 + B_m$ | $2B_m^2 - B_m$ |

With the above results we can compute $F_{i_1,i_2}(\mathbf{0})$, which is always $\pm 2^{m/2}$, and also $\tilde{f}_{i_1,i_2}(\mathbf{0})$, which is in $\{0, 1\}$ depending on the value of $F_{i_1,i_2}(\mathbf{0})$.

Now we put in the following tables the values of $\tilde{f}_{i_1,i_2}(\mathbf{0})$ and $f_{i_1,i_2}(\mathbf{0})$. When these values coincide we conclude that $f_{i_1,i_2}$ is self-dual, otherwise $f_{i_1,i_2}$ is anti-self-dual.

| $\tilde{f}_{i_1,i_2}(\mathbf{0})$ | $m \equiv 2 \pmod 8$ | $m \equiv 6 \pmod 8$ | $f_{i_1,i_2}(\mathbf{0})$ | $m \equiv 2 \pmod 8$ | $m \equiv 6 \pmod 8$ |
|---|---|---|---|---|---|
| $(i_1, i_2) = (0, 1)$ | 1 | 0 | $(i_1, i_2) = (0, 1)$ | 1 | 1 |
| $(i_1, i_2) = (2, 3)$ | 0 | 1 | $(i_1, i_2) = (2, 3)$ | 0 | 0 |
| $(i_1, i_2) = (0, 3)$ | 0 | 1 | $(i_1, i_2) = (0, 3)$ | 1 | 1 |
| $(i_1, i_2) = (1, 2)$ | 1 | 0 | $(i_1, i_2) = (1, 2)$ | 0 | 0 |

□

**Theorem 2.5** *For any even $m \geq 4$ the bent functions $f_{i_1,i_2}$, where $i_1 - i_2 \equiv 1 \pmod 2$ are not of the Maiorana-McFarland type.*

*Proof.* Let us prove the statement by using contradiction. Assume that $f_{i_1,i_2}$ is of Maiorana-McFarland type. This means that a binary variable vector $\mathbf{z}$, of length $m$, can be divided into two subvectors $\mathbf{x}$ and $\mathbf{y}$ of the same length $m/2$ such that

$$f_{i_1,i_2}(\mathbf{z}) = \mathbf{x} \cdot \varphi(\mathbf{y}) + g(\mathbf{y}),$$

where $\varphi$ is a permutation of $\mathbb{F}_2^{m/2}$ and $g(\mathbf{y})$ is some boolean function. Note that $\mathbf{x}$ and $\mathbf{y}$ run over all the $2^{m/2} \cdot 2^{m/2}$ possible values. Consider the set of values of $f_{i_1,i_2}(\mathbf{z})$ when $\mathbf{x}$ runs over all the values in $\mathbb{F}_2^{m/2}$ and $\mathbf{y}$ is fixed to be $\mathbf{y} = \mathbf{y}_0$, such that $\varphi(\mathbf{y}_0)$ is the zero vector. In this case $x \cdot \varphi(\mathbf{y}_0) = 0$ and $f_{i_1,i_2}(\mathbf{z}) = g(\mathbf{y}_0)$ is a constant. Since $\mathbf{x}$ is running over $\mathbb{F}_2^{m/2}$ its weight takes $m/2 + 1 > 2$ different consecutive values. Hence, it takes more than 2 different values of weight modulo 4 and, for all these values, the function $f_{i_1,i_2}(\mathbf{z})$ is constant. This contradicts the definition of the function $f_{i_1,i_2}$. □

# References


[1] T. Beth, D. Junickel, H. Lenz, *Design Theory.* Manheim, Germany: Wiessenschaftverlag, 1985; Cambridge, U.K.: Cambridge Univ. Press, 1986.

[2] Joaquim Borges, Josep Rifà, Victor Zinoviev, "New families of completely regular codes and their corresponding distance regular coset graphs". *Des. Codes Cryptogr.* To appear, DOI: 10.1007/s10623-012-9713-3.

[3] Claude Carlet, Lars Eirik Danielsen, Matthew G. Parker, and Patrick Sole, "Self-dual bent functions." *Int. J. Inform. and Coding Theory*, vol. 1, 384-399, 2010.

[4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977.

[5] Xiang-Dong Hou, "Classification of self dual quadratic bent functions." *Des. Codes Cryptogr.* vol. 63, 183-198, 2012.

[6] P. K. Menon, "On difference sets whose parameters satisfy a certain relation." *Proc. Amer. Math. Soc.* vol. 13, 739-745, 1962.